NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 60495B
1 October 2019

JOHN L YOUNG

Dear Mr. Young:

This further responds to your Freedom of Information Act (FOIA) request of 3 January 2010 for the following documents (cited in the footnotes of NDS DOCID 3417193 provided to you in FOIA Case 60251):

1. Unknown author, Fifty Years of Mathematical Cryptanalysis (Fort Meade), Md. NSA, 1988.
2. DDIR files, 96026, Box 4, Drake Notebook, Proto Paper.
3. Ibid, Unknown Author, draft history of COMPUSEC, in CCH files.
4. Interview, Norman Boardman, by Robert D. Farley, 1986, OH 3-86, NSA.

A copy of your request is enclosed. As stated in our initial response to you, Item 1 of your request ("Fifty Years of Mathematical Cryptanalysis") was processed in a FOIA request received prior to yours. That processing is now completed and the document is enclosed. Certain information, however, has been deleted from the enclosure.

Some of the withheld information has been found to be currently and properly classified in accordance with Executive Order 13526. The information meets the criteria for classification as set forth in Subparagraph (c) of Section 1.4 and remains classified TOP SECRET as provided in Section 1.2 of Executive Order 13526. The information is classified because its disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)). The information is exempt from automatic declassification in accordance with Section 3.3(b)(3) of E.O. 13526.

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in this document. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 3024(i); and Section 6, Public Law 86-36 (50 U.S. Code 3605).

Personal information regarding individuals has been deleted from the enclosures in accordance with 5 U.S.C. 552 (b)(6). This exemption protects from disclosure information that would constitute a clearly unwarranted invasion of personal privacy. In balancing the public interest for the information you request against the privacy interests involved, we have determined that the privacy interests sufficiently satisfy the requirements for the application of the (b)(6) exemption.

Since these deletions may be construed as a partial denial of your request, you are hereby advised of this Agency's appeal procedures.

You may appeal this decision. If you decide to appeal, you should do so in the manner outlined below. NSA will endeavor to respond within 20 working days of receiving any appeal, absent any unusual circumstances.

- The appeal must be sent via U.S. postal mail, fax, or electronic delivery (e-mail) and addressed to:

  NSA FOIA/PA Appeal Authority (P132)
  National Security Agency
  9800 Savage Road STE 6932
  Fort George G. Meade, MD 20755-6932

  The facsimile number is 443-479-3612.
  The appropriate email address to submit an appeal is FOIARSC@nsa.gov.

- It must be postmarked or delivered electronically no later than 90 calendar days from the date of this letter. Decisions appealed after 90 days will not be addressed.
- Please include the case number provided above.
- Please describe with sufficient detail why you believe the denial of requested information was unwarranted.

You may also contact our FOIA Public Liaison at foialo@nsa.gov for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Rd. - OGIS
College Park, MD 20740
ogis@nara.gov
877-684-6448
(Fax) 202-741-5769

Sincerely,

for Shawn C. Lukins

JOHN R. CHAPMAN
Chief, FOIA/PA Office
NSA Initial Denial Authority

Encls:
a/s

From: webteam@nsa.gov
Sent: Sunday, January 03, 2010 9:47 AM
To: FOIANET
Cc: jya@pipeline.com
Subject: Young, John - FOIA Request (Web form submission)

Name: John L Young

Email: jya@pipeline.com

Company: Cryptome.org

Records Requested:
Documents cited in notes of NDS DOCID: 3417193 recently provided to me by NSA:

1. Unknown Author, Fifty Years of Mathematical Cryptanalysis (Fort Meade), Md. NSA, 1988.

2. DDIR files, 96026, Box 4, Drake Notebook, Proto Paper.

3. Ibid, Unknown Author, draft history of COMPUSEC, in CCH files.

4. Interview, Norman Boardman, by Robert D. Farley, 1986, OH 3-86, NSA.

Thank you very much,

John Young

Doc ID: 6649792

~~TOP SECRET~~

Fifty Years of Mathematical Cryptanalysis

CLASSIFIED BY NSA/CSSM 123-2
DECLASSIFIED ON: ORIGINATING AGENCY'S
DETERMINATION REQUIRED

~~Not Releasable To Contractors~~

~~LACONIC~~

THIS DOCUMENT CONTAINS CODEWORD MATERIAL

~~TOP SECRET~~

Fifty Years of Mathematical Cryptanalysis (1937-1987)

by Glenn F. Stahly

August 1988

(b)(1)
(b)(3)-P.L. 86-36

~~SECRET//SI~~

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Contents

~~SECRET//SI~~

[redacted]

~~SECRET//SI~~

[redacted]

(b)(1)
(b)(3)-P.L. 86-36

Preface

Although this paper concentrates on mathematical cryptanalysis, it is by no means intended to disparage the work of or results produced by nonmathematical cryptanalysts, who excel in their own right and frequently produce results that mathematics could not. Many of them work side by side with the mathematicians and often lead them to success by formulating cryptanalytic problems in such a way as to permit the application of abstract mathematics. In fact, they not infrequently succeed in situations where "pure reason" fails the mathematician and leaves him (or her) floundering. But it was absolutely essential during WW II that mathematicians and nonmathematicians work hand-in-glove, and only because of this cooperation were they so spectacularly successful.

Neither is it my intention to suggest that manual cryptography will disappear or even diminish in importance. I believe that will never happen, and therefore we must continue to train and sustain manual cryptanalysts and to provide them with technological support (computers, mathematics, linguistics, and engineering) just as we do the usually more mathematically oriented machine cryptanalysts.

Mathematical cryptanalysis is much more than merely counting letters, adding and subtracting numbers, or computing logarithms. It involves the application to cryptanalytic problems of advanced mathematical subjects such as probability theory, mathematical statistics, group theory, abstract algebra, combinatorial theory, and many more. Some of the world's foremost mathematicians have been connected with cryptanalysis, either as direct practioners (e.g., Alan Turing) or as consultants (e.g., John von Neumann). So also have such outstanding mathematical statisticians as John Tukey.

It is impossible to discuss in this survey any work in mathematical cryptanalysis not done by the United States or the United Kingdom, although we have had glimpses of the capabilities of a few other countries through the opaque windows of Third Party relationships. Australia and Canada, other Second Parties, likewise have made contributions to mathematical cryptanalysis that are not discussed here. We can also assess the cryptographic skills of most foreign nations as we attack their enciphered communications, but it is hard to tell how closely these are connected to their cryptanalytic efforts and even more difficult to guess how or if they use mathematicians.

~~(TOP SECRET//SI)~~ We believe the U.S. and the U.K. are far ahead of the rest of the world in the area of mathematical cryptanalysis, not because of any innate superiority in this area but because the second World War drove home to us the value of mathematics for cryptanalysis. We took that lesson to heart and nurtured the seeds that were planted during the war; consequently, we now have fifty years of experience in applying mathematics to cryptology. We know a great deal about what works and what doesn't, [redacted]

(b)(1)
(b)(3)-P.L. 86-36

faster and better computers, which in turn stimulated new and better cryptomathematical techniques.

Today there is world-wide interest in mathematical cryptology, with academic mathematicians slowly but surely discovering our secrets and publishing them openly. In the process they are also high-lighting the fact that mathematics has much to offer cryptanalysis. Our lead is bound to diminish. I fervently hope that this look at the past will inspire our younger mathematicians and cryptanalysts to stay ahead of the pack, and our managers to help them do so.

UNCLASSIFIED~~//FOR OFFICIAL USE ONLY~~

I am grateful for the patient and efficient assistance of [redacted] in locating documents in the R51 Classified Mathematics Library, which I used extensively. I also made considerable use of the P1 Crypyologic Collection, now located (only temporarily, I hope) with NSA Archives at SAB-2, and I thank the people there for their help. Special thanks are due to [redacted] of P1, who spent a great deal of time showing me how to convert my computer files to OfficeWriter format, correcting many of my mistakes, and then printing the final version of this paper for me.

(b)(3)-P.L. 86-36

Fifty Years of Mathematical Cryptanalysis (1937-1987)

I. Introduction

A. Background

The driving forces behind the development of mathematical cryptanalysis in the last 50 years have been twofold: the critical need for intelligence during WW II and since; and the tremendous pace of technological growth in the communications and computer fields. Intelligence requirements, of course, have led to the provision of the manpower and monetary resources that make it possible to mount sophisticated cryptanalytic attacks. Technology has both created the cryptanalytic problems and provided the means to attack them, and the particular forms taken by technological building blocks used in cipher machines have shaped the directions of cryptomathematical research. This paper is a survey of the development of mathematical cryptanalysis and its relationship to technology.

The history of manual cryptology, essentially the only form of cryptology in existence until the era between the world wars, appears to be a succession of rather specific new systems followed by "general solutions" of them. Some general principles did emerge (e.g., the use of characteristic letter frequencies as described by Edgar Allan Poe in "The Gold Bug"), but by and large cryptanalytic science consisted of ad hoc solutions to specific cryptographic systems. This was true also for the Wheatstone and Kryha mechanical cryptographic devices, but with the advent between World Wars I and II of such generic electromechanical cryptographic components as "wired wheels" and "pin wheels" came also the opportunity and necessity to develop generic cryptanalytic principles. Of course, each specific implementation and each particular usage of a general cryptographic principle require some specific modification of the general attack on it, but nevertheless there are basic approaches to wired wheel problems that are quite different from the basic approaches to pin wheel problems. The basic approaches to shift register cryptanalysis and to presently emerging cryptographic techniques differ from both of these.

B. Technology

Hitler's new warfare techniques (the Blitzkrieg), developed between the first and second world wars, demanded new command and control capabilities, and radio communication technology was ready to do the job if adequate cryptographic security could be maintained. The Germans believed the commercial ENIGMA electromechanical cipher machine could be improved enough to satisfy tactical requirements, and committed themselves to that course. They later developed electromechanical teleprinter cipher machines (TUNNY and STURGEON) for higher-level communications. The United States, over the objections of William F. Friedman, used for some field communications a modified version of the C-38, called the M-209 (Army) or the CSP-1500 (Navy), that was built in this country under an agreement with Boris Hagelin, inventor of the C-38.

Our high-level cipher machine was the electromechanical SIGABA, which was based on wired wheels. ENIGMA, TUNNY, and the Hagelin machines were all read and exploited during the war, but (apparently) not SIGABA.

Sophisticated mathematical and cryptanalytic techniques were developed to attack ENIGMA and TUNNY, but without the technology to build bombes and COLOSSI (the plural of COLOSSUS) they would have been useless (see sections IIA and IIB). The COLOSSI went beyond the state of engineering art at that time, and some people said they could never be made to work. The bombes were largely electromechanical with some vacuum tube electronics, while the COLOSSI had a few thousand vacuum tubes and some electromechanical components. COLOSSI were put together under the exigencies of war-time pressures by some of the best engineers in England (and later here), and they did in fact work. They appear to be the "missing link" in the evolution of computers from theory (a la Charles Babbage) to EDVAC (the first programmable general purpose machine); see [190] and [121].

[redacted]

(b)(3)-P.L. 86-36

By the late 1940's, communications technology had progressed to the point that faster and more automatic cryptography was needed. [redacted] has written a superb review, [88], of U.S. efforts to meet that need, covering roughly the years 1950 to 1980. He emphasizes the interaction of electronic technology and COMSEC design, the other side of the coin from the emphasis of this paper, but since cryptographic design and cryptanalysis are inseparable his paper is full of insights that are invaluable for SIGINT cryptanalysts and COMSEC designers alike.

UNCLASSIFIED [redacted]

(b)(3)-P.L. 86-36

[redacted] recalls that early U.S. electronic cipher machine designs were greatly influenced by previous electromechanical cipher equipment, a state of affairs observed elsewhere (see the last paragraph of Appendix IV). Electronic technology in the 1940's was based on vacuum tubes, which could not easily be used to emulate wired rotors. Pin wheels were another matter; tubes containing multiple anodes arranged in a circle were well adapted to simulate banks of pin wheels. Moreover, much greater flexibility for controlling the stepping of such "wheels" was available with electronic logic.

[redacted]

A major project was therefore initiated to make an abstract mathematical study of "rules of motion". Some American university mathematicians were put under contract to assist in this research, among them S.S. Cairns, an outstanding number theorist then at the University of Illinois. John Koken, one of his students, studied stepping rules [redacted]

[redacted]

(b)(3)-P.L. 86-36

and a number of U.S. cipher machines were designed to use "Koken" registers, as they were called in this form.

[redacted]

At the same time, general purpose electronic computers were being investigated for cryptanalytic applications and NSA (actually its predecessors) was soon heavily involved in computer design, [181], [211]. William F. Friedman had introduced IBM punched card machinery into cryptanalytic and cryptographic operations before WW II, and it was heavily (and ingeniously) used by Army cryptanalysts throughout the war, [10]. A 1955 study, [143], by the NSA R&D organization indicated that COMINT requirements for analytic equipment had grown by a factor of about one million since 1945. Since then communications volumes and speeds have increased manyfold with new electronic technology and new techniques being introduced almost continuously. This puts great pressure on designers of cryptography, who today must somehow produce key bits at rates approaching billions per second, and also on cryptanalysts, who must analyze similar volumes of data. Computer designers have used the same technological advances in electronic circuitry to develop machines that can do billions of binary operations per second, and cryptanalytic mathematicians have used such capabilities to develop new attacks on modern cipher machines. Each new generation of supercomputers elicits genuinely new ideas for attacks (not merely the faster implementation of old ideas, although that surely takes place also); cryptanalysts typically stretch to the limit the capabilities of any new tools they can obtain as they grapple with previously intractable problems.

The increased speed of electronic components has been accompanied by decreased cost, with the result that many countries can now afford to design and build their own cryptographic machines whereas they previously purchased commercial cryptography. Moreover, many more commercial cipher machines are offered for sale today by many more companies than ever before. This means that today's machine cryptanalysts can no longer concentrate on a few known cryptographies, but face instead an array of nearly 300 commercial machines which may be used by our targets, and an ever increasing number of indigenously designed (and therefore unknown) cryptographies. It is also true that more forms of information are being transmitted today; cryptanalysts have to deal not only with record traffic ("messages") but also with speech (both analogue and digital), facsimile, computer data, telemetry, video, and other esoteric types of data.

Ronald Rivest of MIT believes, [193], that today's computing technology gives the cryptographer an overwhelming advantage over the cryptanalyst, and argues his thesis by means of an example. In my opinion, he is partly correct, but his approach is entirely too simplistic and ignores the realities of protecting high-speed, high-volume communications systems. It is nevertheless true that modern technology is making cryptanalysis much more difficult than ever before.

C. Mathematics

(b)(3)-P.L. 86-36

[redacted] Early in his career William F. Friedman consciously set out to systematize cryptology, and he laid the foundations of mathematical cryptanalysis not only by his own work and writings (though he was not a mathematician) but by hiring mathematicians (e.g., Solomon Kullback and Abraham Sinkov) among his first assistants when the Army's Signal Intelligence Service was set up under his leadership after Yardley's Black Chamber was disbanded in 1930. This trend was given added emphasis during the years of World War II because a number of noted mathematicians (and some who were to become noted) wisely were drawn into cryptanalytic work, such men as Alan Turing, W.T. Tutte, I.J. Good, and Shaun Wylie in England, and [redacted] Marshall Hall, Jr., and Robert Greenwood in the U.S., to name a few. (See paragraphs A and B of Appendix I for a probably incomplete list of mathematicians who worked in cryptanalysis during the war.) Moreover, it was the pioneering work of the Polish mathematician Marian Rejewski, [192], that was responsible for the later British and American successes against ENIGMA (see paragraph A of Section II). It has turned out, of course, that cipher machines are particularly susceptible to mathematical analysis (although they aren't always solved or exploited), and the work of these men firmly established the value of mathematics in cryptanalysis.

The outstanding contributions to cryptanalysis made by these mathematicians caused both the United States and England to recognize the need for continued mathematical assistance to that discipline. Accordingly, following the merger of the U.S. Armed Forces that took place shortly after the war, the Armed Forces Security Agency (AFSA, which became NSA in 1952) established in 1951 the Special Cryptologic Advisory Group (SCAG) composed of about twelve prominent scientists including the mathematicians S.S. Cairns, J. von Neumann, C.B. Tompkins, C. Shannon, and H.P. Robertson. This group was reorganized in Jan 1953 and renamed the NSA Scientific Advisory Board (NSASAB) with S.S. Cairns acting as chairman, [15]. A year later NSASAB suggested that three panels be formed under its aegis, and these were subsequently established. One of them was the Mathematics Panel, which continued in operation until it was disestablished by then Director Admiral Gayler in 1970. Reference [15] contains a list of mathematicians who had served on the Mathematics Panel up to 1965; it is reproduced in paragraph C of Appendix I. Recommendations of the Panel were taken seriously and many were implemented; such actions include the initiation of the NSA Technical Journal and the formation of the CryptoMathematics Institute. Panel members were also of great assistance in our efforts to recruit mathematicians.

~~UNCLASSIFIED~~

At about the same time that SCAG was formed, NSA also embarked on a recruitment program for mathematicians to supplement those who stayed with the Agency upon leaving military service. Some 70 were recruited in 1951 by such mathematicians as Marshall Hall, Jr., and [redacted] [redacted] who had been recalled to active duty during the Korean conflict. Most of these new people had Masters Degrees in mathematics, and about half survived a clearance process that for the first time included the polygraph. This group, known as the Junior Mathematicians, has made outstanding contributions to cryptomathematics. However, the project was a one-shot effort and it was not till 1963 that a continuing hiring and training program for mathematicians was established (in the interim there was uncoordinated but fairly generous direct hiring of mathematicians by various elements of NSA). A list, derived from memory, of those Junior Mathematicians who were finally cleared is contained in paragraph E of Appendix I. Nearly all have now retired.

In 1952 NSA also initiated what was to become the annual SCAMP (for Special Committee Advising in Mathematics, with "P" added for effect; see [61], p. 3) program, a project in which prominent mathematicians are cleared and brought together for a few months in the summer to work on difficult cryptomathematical problems arising at NSA. A great quantity of high quality work and many useful ideas flow from this project, as well as contacts valuable in recruiting mathematicians for full time employment. Appendix I lists the nongovernment mathematicians who attended the first SCAMP session.

[redacted] A few years later, in 1959, NSA established a "captive" think tank, the Communications Research Division of the Institute for Defense Analyses (IDA-CRD), located in Princeton, N.J., [152]. Many prominent mathematicians, among them A.A. Albert, J. Barkley Rosser, Gustav Hedlund, [redacted] and Donald Knuth, have worked at IDA-CRD on temporary (one or two year) appointments and a number of equally talented ones are there on permanent appointments. IDA-CRD has administered the SCAMP program since about 1960. Such general cryptanalytic techniques [redacted] as well as a number of specific cryptanalytic successes produced by IDA-CRD, have amply repaid the investment.

(b)(3)-P.L. 86-36

Through the efforts of Frank Raven, 1963 saw the beginning of the P1 Cryptologic Mathematician Program in which 20 to 30 high-quality mathematicians are hired each year to enter a three-year program of combined on-the-job training tours and formal classroom training in the applications of mathematics to cryptanalysis. Most of these mathematicians come to NSA with Masters Degrees; some have Doctorates and some have only Bachelors Degrees. This program has been a remarkable success, with graduates now working in all parts of this Agency, including executive management levels.

The Junior Mathematicians and the Cryptologic Mathematician Program have not been the only sources of mathematical talent for NSA; fewer than half the Agency's mathematicians belong to these groups. The others have come as direct hires to R5, X1, G4, A5 (or to predecessors of these), and to a few other organizations, and they too have made significant contributions to mathematical cryptanalysis over the

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

years. It should also be pointed out that mathematical statisticians are included in the term "mathematicians" throughout this paper. Solomon Kullback (a previous DDR for NSA) and John Tukey (a one-time consultant for NSA) are among a number of noted mathematical statisticians who have contributed to cryptology.

(b)(1)
(b)(3)-P.L. 86-36

[redacted] [redacted]

We believe that at the present time NSA is the largest employer of mathematicians in the world. At the end of 1987, there were 273 persons with Bachelors Degrees in mathematics, another 245 with Masters Degrees, and 69 more with Doctorates for a total of 587 persons working at NSA with the job title "Mathematician"; most were actually doing or supporting mathematical cryptanalysis. There was also a sizeable number of persons with advanced degrees in mathematics holding other job titles such as "Computer Scientist", "Manager", or "Cryptanalyst".

D. Public Cryptologic Research

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted] The 20 years from 1950 to 1970 saw the development of a large body of mathematical theory relating to cryptologic aspects [redacted] Then the introduction of the Data Encryption Standard (DES) by the National Bureau of Standards caused a controversy that focussed public attention on the cryptologic work of Whitfield Diffie and Martin Hellman, [86], (especially on their rediscovery of nonsecret encryption, which they call public key cryptography), thus triggering extensive interest in cryptology among research mathematicians all over the world. Also, the increasing importance of coding theory for communications technology has fueled a great deal of mathematical research in that field, which turns out to overlap cryptanalytic shift register mathematics to a considerable extent (see Chapter 4 of [197]). Several recent papers and books (e.g., [196]) show that our previously [redacted]

New principles are already evident in emerging commercial cipher machines, and there is much foreign interest in the annual conferences now devoted to cryptology. In addition, public key cryptography was independently discovered by university mathematicians, [86], several years after GCHQ's James Ellis first conceived it in 1970, [92]. The idea has led to new areas of mathematical cryptanalysis that will be needed for operational problems in the future as foreign cryptographers begin to use public key systems. The fact that these areas are being actively studied and results published in the open literature will make it much more difficult for NSA cryptomathematicians.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Another aspect of today's technology that will greatly affect cryptology is the rapidly increasing power and decreasing cost and size of microprocessors. Many new cipher machines today are based on microprocessor chips, which means that the cryptography is in software form and can thus be changed easily and inexpensively (and frequently, if desired). Whereas cryptography implemented in hardware can be expected to remain in use for quite long periods of time hence justifying some time and expense to develop attacks, software cryptography can be replaced overnight which means that attacks must be developed under time pressure, if at all; it may not even be cost effective to attack usages of software cryptography that change too frequently. On the other hand, it is more difficult than most people realize to devise secure cryptography and therefore we may expect frequent software changes at least occasionally to produce highly exploitable systems. Identifying and diagnosing them will be the problem.

E. Prognosis

Mathematical cryptanalysis is in a time of transition caused by technological changes in hardware and by unprecedented public interest in cryptology. Huge volumes of enciphered communications are on the air today and volumes are increasing exponentially, providing more opportunities for cryptanalysis than ever before. Of course, formidable obstacles must be overcome in order even to mount cryptanalytic attacks: collection technology must be developed to cope with these volumes; methods to select vulnerable transmissions must be devised; signal analytic technology must be modernized; and adequate numbers of mathematicians and cryptanalysts must be trained to deal with tomorrow's problems. But that is ever the position of cryptanalysts -- lagging just a few steps behind communications and cryptographic technology!

UNCLASSIFIED

On the other hand, technology is a two-edged sword. Supercomputers of every generation have been eagerly embraced by cryptanalysts; in fact, cryptanalytic needs have driven the development of computer hardware technology and are largely responsible for the U.S. lead in that field, [211]. Too, special purpose machines have been built (e.g., the bombes of WW II, or [redacted] The challenge is for cryptemathematicians to remain no more than a few steps behind the cryptographers.

(b)(3)-P.L. 86-36

II. Mechanical and Electromechanical Cipher Machines

The history of cryptology up to the second World War has been very nicely summarized by William F. Friedman in a series of six lectures presented to NSA employees; these were published in 1963 and later reissued as [107]. In the last of his lectures Friedman discussed, rather sketchily, a number of mechanical cryptographic machines such as the Wheatstone manually-operated device and the Kryha spring-driven device. Neither of these was really secure and neither gave rise to any significant general cryptanalytic techniques. Friedman then discussed the development of wired wheel cryptography, particularly that which took place in the United States. He also described the Hagelin B-21 and M-209 devices (the M-209 is the U.S. Army designation of a machine produced for Army field use; it is nearly identical with the commercial Hagelin C-38 device described in Appendix IV). Friedman made no mention of the Japanese PURPLE machine, nor, indeed, of any Japanese machines (see [49]), probably for reasons of security, for the need-to-know principle was observed quite rigorously in the early 1960's. Neither did he mention the German TUNNY or STURGEON machines, although he did discuss Gilbert Vernam's invention in 1917 of one-time tape teleprinter cryptography (see also [175]).

(b)(3) - P.L. 86-36

[redacted]

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

B. Teleprinter Cipher Machines

This category contains the German SZ-40 and SZ-42 on-line cipher machines (called TUNNY by the British during WW II) that are described in Appendix III and [11]; the German T-52 series of on-line cipher machines (called STURGEON) described in [219]; and a variety of U.S.

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3) 18 USC 798
(b)(3) 50 USC 3024(i)
(b)(3) P.L. 86-36

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3) 18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36

III. Electronic Cipher Machines

No single electronic cipher machine, nor even a small group of them, seems to be responsible for the development of any significant body of cryptanalytic theory. Rather, it is the generic technology itself that has shaped the course of cryptanalysis of such machines (see Appendix V for an example of electronic cryptography).

[redacted]

There are at least two reasons for this. First, the theory originated in U.S. and British COMSEC studies that began before any electronic cipher machines even existed and continued throughout the developmental phases of a number of equipments. Much of it led to design revisions before production began and so cannot be attributed to anything that was ever actually built. A considerable portion of the theory grew out of abstract mathematical research not specifically related to anything tangible. [redacted] [redacted] paper, [88], is an excellent presentation of the way in which electronic technology shaped U.S. COMSEC and, thus, the cryptanalysis of electronic cipher machines.

[redacted]

[redacted]

[redacted]

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3) 18 USC 798
(b)(3) 50 USC 3024(i)
(b)(3) P.L. 86-36

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3) 18 USC 798
(b)(3) 50 USC 3024(i)
(b)(3) P.L. 86-36

[redacted]

b)(1
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i
(b)(3)-P L 86-36

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3) 18 USC 798
(b)(3) 50 USC 3024(i)
(b)(3) P.L. 86-36

[redacted]

IV. Other Techniques

There are a number of cryptomathematical techniques and theories that were not developed in connection with specific cipher machines (and some that were developed within compartmented problem areas whose details cannot be discussed here) that I believe are important enough to mention in this paper. As NSA's mathematical population grew over the years, the amount of classified cryptomathematical activity increased and diversified so much that it is now extremely difficult to survey it comprehensively. I have therefore tried to identify mathematical developments that are general and will have or have had lasting technical consequences for cryptanalysis. I have included also several techniques important to data processing in general, such as sorting, whose cryptanalytic applications have warranted considerable classified development internally. Most of the above can be categorized as either statistical methods or algorithms, although there are a few which it is more convenient to consider separately.

Statistical and probabilistic questions and methods pervade cryptanalysis. The cryptanalyst continually wants to know how likely some observed or hypothesized event is, or where to set thresholds for statistical tests, or how to program a computer to recognize plain text; the variations are endless. These questions nearly all relate to the results of manipulations of data (i.e., algorithms) carried out or to be carried out by the cryptanalyst or by a computer. To call certain cryptanalytic techniques "statistical" while others are called "algorithms" is thus largely a matter of emphasis and personal taste. Nearly all statistical cryptanalytic techniques involve algorithmic features and most cryptanalytic algorithms have some statistical features. My judgments in this matter have resulted in the following categorizations.

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

Three years later in 1938, Solomon Kullback, one of Friedman's first proteges, published his pioneering work "Statistical Methods in Cryptanalysis", [142], which has now been declassified and is available to the public from Aegean Park Press. In it Kullback sketches some general aspects of probability and statistics, describes briefly a few probability distributions of interest mainly to manual cryptanalysts, and then discusses a number of cryptanalytic applications of these notions (he uses some concepts [redacted] [redacted]. He also includes a great many tables and charts, such as plain text frequency data for several languages and graphs of the Poisson distribution for various parameter values. This may well be the first formal cryptomathematical work by an American professional mathematician or mathematical statistician, conceivably the first by one of any nationality.

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3) 18 USC 798
(b)(3) 50 USC 3024
(b)(3) P.L. 86-36

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted] ~~TOP SECRET UMBRA LACONIC NOCON~~

[redacted]

B. Algorithms

[redacted] An algorithm is an explicit step-by-step method for accomplishing some specific task, a method that can be built into a machine or programmed on a computer. [redacted]

[redacted]

~~TOP SECRET UMBRA LACONIC NOCON~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3) 18 USC 798
(b)(3) 50 USC 3024(i)
(b)(3) P.L. 86-36

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024,
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3) 18 USC 798
(b)(3) 50 USC 3024(i)
(b)(3) P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

V. Computing Power

Cryptanalysis has always required enormous investments of time and effort for data manipulations and for computations of both numerical and logical types. At one time they were carried out with pencil and paper (charcoal and cave walls?), but as cryptographic systems became more complex and communications became more voluminous it was necessary to turn to machines to perform these functions. Sometime around 1935, William F. Friedman introduced the use of IBM punched card equipment for cryptanalysis (and also for the construction of codebooks for U.S. use), and during WW II special purpose hardware appendages were fitted to some of these machines in spite of IBM prohibitions against such tinkering; see [10]. Many machines were also constructed during the war to make frequency counts, compare streams of data, etc., [210], besides the now highly publicized bombes and COLOSSI. Except for the IBM punched card equipment, these were all special purpose devices. Immediately following the end of WW II, attention was drawn, [181], to the possibility of using the emerging digital computers for cryptanalysis. That possibility was made reality by the foresighted cryptanalysts and cryptologic engineers of the time (see [209] and [211]), not only benefitting NSA but in the process giving the United States the lead we now enjoy in computer technology.

A. Special Purpose Devices

UNCLASSIFIED/~~[illegible]~~

(b)(3)-P.L. 86-36

The term Special Purpose Device (SPD) is used at NSA to refer to any machine built to perform a specialized task, usually one related to cryptanalysis. Perhaps the first SPD was the original Polish cyclometer, [192], an electromechanical device built by Poland in the mid-1930's to assist in making a catalog which enabled the Poles to recover daily keys for German Army ENIGMA traffic (the cyclometer exploited weaknesses of the Grundstellung indicator system). This device was followed by the Polish bomby (plural of bomba) and the British bombes (see paragraph A of Section II), both used to exploit the ENIGMA. Later in [redacted]

During the war there were constructed a wide variety of relatively small SPDs to do such "general" special functions as making frequency counts of various kinds (input being supplied usually on punched paper tape), combining two data streams (e.g., forming the bit-by-bit mod 2 sum of two teleprinter messages), etc. Such machines were called analytic aids. A number of SPDs were also built to perform decryption operations once all cryptovariables had been recovered; these were analogues of the cipher machines or systems used by the actual German or Japanese communicators.

[illegible]

[redacted]

(b)(3)-P.L. 86-36

(b)(1)
(b)(3) - P.L. 86-36

[redacted]

CONNIE was a photoelectrical comparator of punched paper tapes. The first model was delivered in Jan 1948 for experimental use [redacted] It operated at 5000 characters per second.

Two ROBINs began operating at NSA (really AFSA at the time) in 1951, [29], and the plan at that time was to acquire several of them to handle all our requirements. They, too, were photoelectrical comparators and also ran at a speed of 5000 characters per second. [redacted]

[redacted]

With the introduction of digital computers into cryptanalytic operations in the early 1950's came predictions of the demise of SPDs. However, the supercomputers of any generation have never been fast enough to cope with all the cryptanalytic problems of their era. In some cases, breaking a message in a particular system requires far too much work even for the computer to do in any reasonable time; in others, the number of messages in a particular system is so great that breaking them all would occupy the computer to the exclusion of other work; in still other cases an SPD is so cheap that using a computer would not be cost effective. Most importantly, a requirement for timely decryption of messages in certain cipher system usages may preclude waiting for computer solutions even though the work would not overload the computer. The answer in any case (assuming the problem has high enough priority) is to build a special purpose computer designed to attack the specific problem in question. The bombe is such a machine, as was COLOSSUS (although COLOSSUS turned out to be much more flexible than anticipated).

[redacted]

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

Analytic aid SPDs have now been largely superseded by remote terminals connected to general purpose computers of various sizes and, more recently, by desktop computers. Analogue SPDs used solely for decryption have also for the most part been replaced by terminals and/or personal computers.

B. Digital Computers

It was in 1946 that Lt. Cdr. James Pendergrass wrote the memo [181] recommending that digital computers be acquired for cryptanalytic uses. The Navy approved the proposal and embarked on the development of what became ATLAS I, the first general purpose computer to be used on cryptanalytic problems, [103]. Much of the design philosophy and many of the machine instructions were heavily influenced by cryptanalytic considerations, and these in turn have influenced computer design to this day. Computers were invented mainly for scientific number-crunching calculations, and might have developed quite differently had not cryptanalytic applications been injected in those early years.

In fact, the ATLAS I and ATLAS II computers were specified by an NSA predecessor and built for it by a company called Engineering Research Associates (ERA) that had been set up specifically to build "cryptographic analytic equipment" for the government, [222], (ATLAS II subsequently was marketed commercially as the UNIVAC 1103). ERA was formed in 1946 by Howard T. Engstrom (later a Deputy Director of NSA) and William C. Norris (later president of Control Data Corporation, now retired) with the help of Ralph I. Meader and the backing of John E. Parker. It was soon bought by RemRand which later merged with UNIVAC, and still later many of the best technical people left to form Control Data Corporation which in turn spun off Cray Research, Inc.

Sam Snyder, one of Friedman's early recruits, has written an excellent history, [211], of NSA general purpose computers covering the period from 1945 to 1964. In this present paper I will attempt merely to identify some of the highlights of that period and since that are relevant to cryptanalysis.

Our first computers were programmed in absolute machine language (using octal numbers) by persons who "learned while doing". Debugging was done in real time at the console of the computer itself. It was a great advance when assembly languages were introduced by IBM in the mid to late 1950's, but it was a blow to NSA programmers when in 1957 or 1958 they were no longer allowed to debug at the console; instead, computer operators ran the programs and gave them a memory dump (in octal numbers!) for debugging purposes.

[redacted] In this same time frame some experiments were being carried out in providing remote terminal computer access to cryptanalysts, resulting in a series of systems: ROGUE, which used ALWAC III; ROB ROY, which used BOGART; and RYE, [182], which initially used UNIVAC 490's that were upgraded later to UNIVAC 494's. These services were furnished mostly to manual system cryptanalysts, [redacted] also employed them profitably. They were intended to satisfy one of the most important requirements of the analysts -- easy access to computing power.

Machine cryptanalysts depended primarily on the main-frames, the supercomputers of their day. They, too, required easy access, and in the late 1950's and the 1960's that really meant they wanted programs to be written quickly; there just was no practical way to give analysts hands-on access to the computers. To get programs written in a hurry, most analysts learned to program in assembly language and then (sometime in the early 1960's) in FORTRAN or even COBOL. Open-shop programming, as this was called, became officially sanctioned at about that time and efforts were made to provide four-hour turn-around time for debugging runs of FORTRAN programs. All these transactions, as well as those for operational runs, were conducted "over the counter"; card decks with programs to be debugged or data to be run were taken to a counter located in T spaces (it was not then named T, of course) where they were logged in and passed on to computer operators. After they were run, the magnetic tape output was carried to line printers where it was queued up according to priority to await printing. Bookbreakers' output, which was often quite lengthy and thus had low priority, sometimes was not printed for weeks. This kind of access to computing power was not ideal for cryptanalysis.

In early 1962, HARVEST was delivered by IBM after eight years of study and development (for the story of HARVEST, see pp. 26-43 of [211]). It was a general purpose computer constructed of proven hardware technology but with such innovative design features as instruction look-ahead, streaming capabilities, and many others. The concept of operations was a step backwards, from a cryptanalyst's point of view. The original idea was to treat HARVEST as a factory running on a 24 hour turnaround cycle, so that one would submit jobs over the counter and get the results 24 hours later. In the event, it was not operated quite that way, but was still too inaccessible to use easily for cryptanalytic research purposes.

Meanwhile, IDA-CRD (which was established in 1959) had in 1960 acquired its first computer, a CDC 1604, and was developing an operating system specifically designed to give researchers the easiest access possible. Any person on the technical staff could take his program deck to the card reader and read it into the computer (or rather into the disk file that served as an input buffer). Facilities were available so that he could monitor the status of the run whenever he wished, and when it was completed the output was automatically printed on the line printer.

[redacted]

As plans were made to upgrade IDA-CRD's 1604 to a CDC 6600 (that year's supercomputer), the decision was made to do away with card decks and use instead the then new cathode ray tube (CRT) terminals for interactive program input and control of input data from disk storage. Thus was born IDASYS, which featured the first-of-its-kind full screen text editor and permitted a researcher to sit at a CRT to write programs which could then be compiled and run at the push of a button. Turnaround time was a matter of seconds for a compilation, not the minimum of four hours required for over-the-counter transactions. The CDC 6600 began running at IDA-CRD in the summer of 1967, and even the most dyed-in-the-wool conservative (i.e., Glenn Stahly) soon abandoned the "security" of his card decks. Reference [68], pp. 2-5, gives a brief outline of IDA-CRD's computer history.

[redacted] Within a year or two A5 (the Soviet problem) and G4 [redacted] under the influence of the demonstrated effectiveness of the IDA-CRD operating system, sought and acquired CDC 6600 and/or 7600 computers dedicated to their own problems, and installed IDASYS which then evolved into the splendid NSA FOLKLORE operating system. From these initial installations have grown the present CAP, CAR, and TCAP complexes. As cryptanalytic problems have grown in volume, diversity, and complexity, so the computer power has been increased by acquiring more computers and ever more powerful ones. Historically, computer power for A5 and G4 has approximately doubled every two years since 1970, and it is estimated that this rate of increase will have to continue for the foreseeable future if requirements are to be satisfied. Additional growth in computer resources beyond this rate of increase is needed now for W (signals analysis), for B6 (the exploding PRC problem), for X1 (COMSEC evaluations), and for R5 (research).

In the 1980's, besides the present supercomputers, technology for networking and for powerful desktop computers has emerged, making it technically possible to fulfill every cryptomathematician's dream of having supercomputing power available at his or her own desk. That takes money, though, and it will be a few years before the dream is fully realized, but NSA is moving (slowly) in that direction. Considerable numbers of personal computers (PCs) are now present in working spaces, local area nets (LANs) are in place in a few offices, and plans are being considered for making the supercomputers accessible to the PCs via networking. One of the large roadblocks is the problem of providing adequate computer security features, a problem far from solved at the time this paper is being written.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VI. Public Key Cryptography

Almost all known public key cryptosystems (see Appendix VII) are mathematical in nature, depending on transformations that are difficult to invert in general. Some public researchers have asserted that the discipline called computational complexity (reference [111] contains a good introduction to complexity theory) is basic to the understanding of public key methods, and that NP-hard problems should be used as the basis for such systems. For instance, the general knapsack problem is known to be NP-complete (and therefore hard in general), and thus should lead to a good public key cryptosystem according to this philosophy.

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VII. COMSEC

[redacted] In the evaluation of U.S. and British cryptosystems, both newly proposed ones and those already in use, COMSEC analysts of course consider all the techniques previously described. [redacted] In addition, there are a number of generic attacks unique to the COMSEC arena. The reasons for this are that U.S. systems today have features different from most of those faced by operational cryptanalysts, and, more important, that COMSEC evaluators must consider types of attacks that may be impractical with today's technology but are likely to become feasible in future years. The future must be considered because cipher machines proposed today, if actually built, are likely to be in use for many years to come. The communications they protect may also need protection for years following the actual transmission of the information, perhaps even after the machines have been taken out of use. Forecasting developments in computing and analytic technology and their future costs is therefore an important COMSEC activity.

[redacted]

[redacted]

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VIII. Summing Up

The past fifty years seem to comprise three cryptographic periods; the electromechanical era, the electronic era, and the computer (or computational) era that has just begun. In the electromechanical era, cipher machines were based on wired wheels and/or pin wheels, components possessing certain properties that led to certain types of attacks to which certain types of mathematics were applicable. More and more sophisticated electromechanical designs evolved over the years, of course, especially in those countries having the most sophisticated cryptanalysts and the most advanced hardware technology. This forced the cryptanalysts not only to develop more sophisticated attacks but also to press for ever faster computing machinery.

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

Although new techniques were needed in each era, it is also true that older methods continued to be applicable to many cryptanalytic problems. Not only did cipher machines of previous eras continue in use well beyond the introduction of newer ideas, but some of the newer systems were vulnerable to classical methods. Moreover, at the present time we find that cryptanalytic techniques are required to solve problems in other fields, notably in signals analysis where modern communications technology has turned the business of characterizing complex and previously unseen signals into a cryptanalytic task.

It seems clear that cryptanalytic advances over the years have always stemmed directly from cryptographic advances and that their forms have been dictated both by the technology (in the forms of hardware, software, and algorithmic design) involved in the cryptography and by the technology available for manipulating data and performing computations. I have found no evidence of cryptanalytic techniques being developed in the absence of concrete COMSEC or SIGINT cryptanalytic problems. In the present environment, I believe we can best prepare for the future by increasing our level of mathematical and computational expertise and by closely monitoring technological developments in these areas and in the domain of public cryptologic research.

We have already taken one step that should help us maintain our cryptanalytic leadership; [redacted] However, we ought also to make sure that NSA acquires the requisite mathematical resources to keep up with (at a minimum) or stay ahead of (if possible) the public cryptographers and those targets which may take advantage of all the public work, as well as with the broadening range of application of cryptanalytic methods.

(b)(3)-P.L. 86-36

Appendix I: Mathematicians in Cryptology in the 1940's and 1950's

A. British Mathematicians in WW II Cryptology

1. In his book "GCHQ", [227], Nigel West mentions a number of British mathematicians who worked at GCHQ during World War II. It is obvious that he has not identified all the mathematicians involved in cryptanalysis at that time, and he may well have thought some persons to be mathematicians who were in fact trained primarily in another field. [redacted] Here are the names of those West calls mathematicians:

Alexander Aitkin, "Professor of Mathematics at Edinburgh University" (p. 153), [redacted]

(b)(1)
(b)(3)-P.L. 86-36

Harold Fletcher, "the Cambridge mathematician" (p. 180);

I. J. Good, "Cambridge mathematician", (p. 153), "later Professor of Statistics at West Virginia" (p. 268);

Peter Hilton, "later Professor of Mathematics at Cornell University" (p. 191);

John Jeffreys, "Downing College", one of "three distinguished mathematicians from Cambridge" (p. 128), [redacted]

Dillwyn Knox, "a talented, if unorthodox, mathematician" (p. 90-91), [redacted]

George McVittie, "later Professor of Mathematics at London University" (p. 205), [redacted]

Donald Michie, "later Professor of Machine Intelligence at Edinburgh" (p. 191);

M. H. A. Newman, "University Lecturer in Mathematics at Cambridge" (p. 191);

Alan Turing, "King's", one of "three distinguished mathematicians from Cambridge" (p. 128);

W. T. Tutte, one of "the mathematicians" (p. 191);

Gordon Welchman, "Sidney Sussex College", one of "three distinguished mathematicians from Cambridge" (p. 128);

John H. Whitehead, "later Professor of Pure Mathematics at Cambridge" (p. 192);

Shaun Wylie, "brilliant topologist" (p. 191).

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

[redacted]

[redacted]

B. American Mathematicians in WW II Cryptology

1. In 1946 the U.S. Navy published the technical papers produced by an OP-20-G research group that worked on ENIGMA problems during the war ([31] is one volume of the series). The following names of authors were found among those papers, with little indication of which ones were mathematicians. In some cases, no first names or even initials were given. Some of them are well known in NSA circles (e.g., Eachus, Wray, et al.), but others are complete mysteries. Here is the list:

Howard H. Campaigne (later with NSA);

Church;

A. H. Clifford;

G. F. Cramer (later with NSA);

Reed Dawson (later with NSA);

Joseph Eachus (later with NSA);

R. B. Ely;

Howard Engstrom (later NSA Deputy Director for R&D);

Gilman;

(b)(3)-P.L. 86-36

[redacted] (later at NSA, and then an NSA consultant);

Robert E. Greenwood (later at NSA, and then an NSA consultant);

[redacted] (later at NSA, and then an NSA consultant);

Robert Hampton, III;

Hanson (may be Eugene Hanson, who attended the first SCAMP);

J. H. Howard;

Dr. H. L. Krall;

Aubrey W. Landers;

Menzel;

Edwin E. Moise;

Pearsall;

W. R. Willis;

W. D. Wray (later with NSA).

2. A cursory search through technical papers of the Army Signal Intelligence Service and some of its successors, for the period during and shortly after WW II, turned up only a few names of authors who had written papers with any mathematical content. Many papers of that time were, unfortunately, not signed or attributed to their authors. The list of Army mathematicians and possible mathematicians is thus quite short:

Jane Brewer;

David Cowan;

Daniel Dribin;

William H. Erskine;

Bernard Gechter;

Walter Jacobs;

Solomon Kullback;

Frank Proschan;

Frank Rowlett;

John N. Seaman;

Abraham Sinkov.

[redacted]

C. Members of the NSASAB Mathematics Panel, to 1965

Reference [15] contains a list, reproduced here, of mathematicians who had served on the Panel up until 1965, the date of the reference (affiliations are as of the last date of Panel service):

A. A. Albert, University of Chicago, still serving in 1965;

[redacted]

(b)(3)-P.L. 86-36

Stewart S. Cairns, University of Illinois, still serving in 1965;

R. P. Dilworth, (Panel Chairman, 1964-65), California Institute of Technology, still serving as panel member in 1965;

A. M. Gleason, Harvard University, still serving in 1965;

Marshall Hall, Jr., Ohio State University, still serving in 1965;

G. A. Hedlund, IDA-CRD, served May 1960 to 1963;

Ivan R. King, University of California at Berkeley, still serving in 1965;

Richard A. Leibler, IDA-CRD, served until 1963;

H. Jerome Keisler, University of Wisconsin, appointed in 1965;

Saunders MacLane, University of Chicago, served until 1961;

Brockway McMillan, Bell Telephone Laboratories, served until 1961;

John Riordan, Bell Telephone Laboratories, served until 1962;

Howard P. Robertson, (Panel Chairman, 1953-54), California Institute of Technology, served until 1961;

J. Barkley Rosser, University of Wisconsin, still serving in 1965;

Claude Shannon, Bell Telephone Laboratories, served until 1958;

C. B. Tompkins, University of California at Los Angeles, still serving in 1965;

John W. Tukey, (Panel Chairman, 1958-64), Princeton University, served until 1964;

John von Neumann, Institute for Advanced Study, served until 1957;

S. S. Wilks, (Panel Chairman, 1954-58), served until 1964.

NSA Executive Secretaries to the Mathematics Panel were:

William A. Blankinship, May 1957-Jun 1961;

Daniel M. Dribin, Jun 1961-Apr 1965;

Ralph W. Jollensten, appointed Apr 1965.

D. Mathematicians Attending the First SCAMP

1. Those nongovernment mathematicians who attended SCAMP 52 (the first SCAMP) were:

A. Adrian Albert, Professor, University of Chicago;

Truman Botts, Asst. Professor, University of Virginia;

Stewart S. Cairns, Professor and Head of Department, University of Illinois (Chairman of SCAMP 52);

Dick Wick Hall, Professor, University of Maryland;

Eugene H. Hanson, Professor and Head of Department, North Texas State College;

G. A. Hedlund, Professor and Chairman of Department, Yale University;

John C. Koken, Research Assistant, University of Illinois;

Richard A. Leibler, Sandia Corporation;

Lowell J. Paige, Asst. Professor, University of California;

A. E. Roberts, Jr., Engineering Research Associates;

Donald C. Spencer, Professor, Princeton University;

C. B. Tompkins, Principal Investigator, Logistics Research Project, George Washington University;

James A. Ward, Professor, University of Kentucky;

Charles Wexler, Professor, Arizona State College.

2. AFSA personnel (most of them mathematicians) at SCAMP 52 were:

Patrick P. Billingsley, AFSA-341 (an R51 predecessor);

Charles Bostick, AFSA-206 (a P1 predecessor);

Jane Brewer, AFSA-412 (a COMSEC element);

Howard H. Campaigne, AFSA-34 (an R5 predecessor);

Reed B. Dawson, AFSA-341;

Daniel Dribin, AFSA-206;

Joseph J. Eachus, AFSA-35 (an R&D element);

(b)(3)-P.L. 86-36

[redacted] AFSA-206;

Bassford C. Getchell, AFSA-206;

Andrew M. Gleason, AFSA-341;

[redacted], Jr., AFSA-34;

Arthur Levenson, AFSA-206;

[redacted] AFSA-14 (possibly a Security element);

Robert H. Shaw, AFSA-412;

[redacted], AFSA-206;

[redacted] AFSA-344 (possibly an administrative person).

(b)(3)-P.L. 86-36

E. Junior Mathematicians of 1951

The Junior Mathematicians were recruited during the 1950-51 school year and entered on duty during the summer of 1951. They were sent first to the Training School, located at that time on U St., NW, in downtown Washington, D.C., and assembled there as a group when enough had appeared. Initial training was provided by self-study courses in cryptography and then elementary cryptanalysis, followed by some courses especially designed for them. In November of that year the group was moved to Arlington Hall Station in Virginia where AFSA (soon renamed NSA) was located.

The planned operational training was delayed, the idea being to wait until all members of the group were cleared; in those days we were hired first and cleared later. 1951 happened to be the first year polygraphs were used as part of the clearance process, and the Junior Mathematicians suffered through the birth pangs of that effort. It turned out, in fact, that about half of the group was eventually denied clearance. However, it was kept intact for a while in hopes of clearing everyone, and because some persons were as yet uncleared it was housed in the basement of the Arlington Hall cafeteria which was seperate from the operations buildings (all were wooden "temporary" structures). There, further self-study cryptanalysis courses, mathematics seminars organized by group members, and occasional lectures from old hands occupied the time.

[redacted] At some point during the winter, it was realized that the clearance process would take forever, and so those who had been cleared were moved to operational spaces where a series of short (two-week) on-the-job training tours were arranged. Then half of the mathematicians were given a series of fulltime courses on the uses of IBM and other data processing equipment while the other half took full-time courses in ENIGMA, STURGEON, and [redacted] cryptanalysis (the plan was for each half of the group to take each series of courses, but that didn't happen). Following this, everyone was deployed to some longer-term cryptanalytic or data processing tour, and in time all were assimilated into various operational organizations.

The following list, derived from memory with the help of Charlie Bostick, Ralph Jollensten, Arthur Levenson, and William Lutwiniak, contains the names of most of the 1951 Junior Mathematicians who made it through the clearance process:

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(6)

[redacted]

Charles Bostick;

Pansy Brooks;

[redacted]

Frank Dresser;

[redacted]

Sydney Fairbanks (not a mathematician);

Lowell ("Jim") Frazer;

[redacted]

Evelyn Garbe;

Fritz Goepper;

[redacted]

Lane Hart, III;

Robert Highbarger;

John Hodges;

[redacted]

Ralph Jollensten;

Richard Kern;

[redacted]

Edward Magnuson;

[redacted]

(b)(6)

Paul Oyer;

Carolyn Palmer;

James Pettus;

[redacted]

Leonard Schlauch;

Marvin Sendrow;

Robert R. Smith

William R. Smith;

Glenn Stahly;

Albert Verbits;

Bernard Witt.

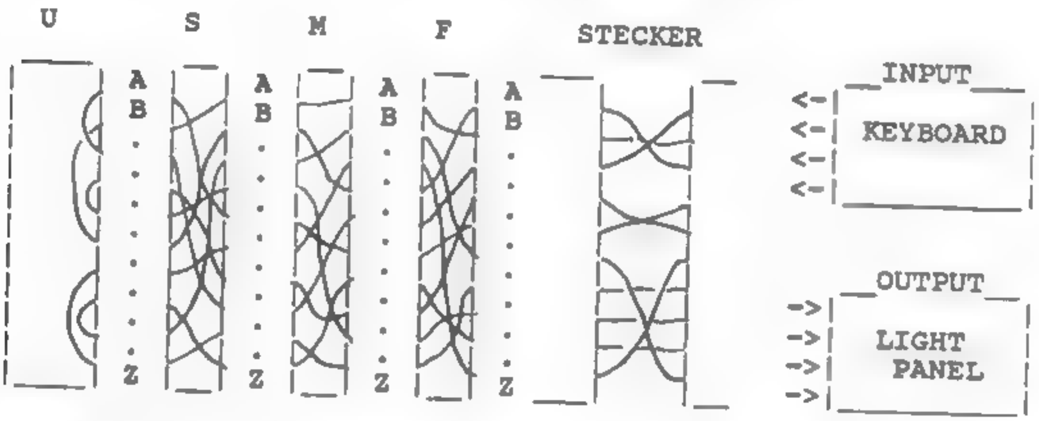
Appendix II: ENIGMA (see [44], [158])

ENIGMA, an off-line cipher machine, was the first wired wheel machine to be used to any significant extent. It appeared in Germany about 1925 as a commercial offering, at which time it had three wheels and a reflector (Umkehrwalze). In 1926 the German Army introduced a version which had different wirings, a different reflector, and a new feature, the plug board (Steckerverbindung, or "stecker") between the wheels and the input-output functions. The Poles attacked the German Army usage and made limited progress by discovering that some form of ENIGMA was being used and that the first six letters of each message were probably indicators. In Oct 1931, the French intelligence services developed a source within the Cipher Bureau of the German Ministry of Defense who supplied them with copies of code clerks' instructions for ENIGMA and, subsequently at regular intervals, with copies of daily key lists (but no wirings).

The French Cipher Service looked at these and immediately declared the machine impossible to solve. French intelligence then obtained permission to give the information to France's allies and to suggest a common attack on the problem. GC & CS (Government Code and Cypher School, the predecessor of GCHQ) was given first chance, but they "filed their copies of the documents" and did not respond to the offer of cooperation. (Gordon Welchman, however, believes the British had more effort against ENIGMA before the war than they indicated to the French; see [6], pp. 71-110.) The French then approached the Poles, who accepted with enthusiasm and promised to share results of their work. However, all cryptanalytic efforts failed. At that point, 1 Sep 1932, those in charge of Polish intelligence brought in three mathematicians, Marian Rejewski, Henryk Zygalski, and Jerzy Rozycki. In the middle of October, 1932, Rejewski was put to work on ENIGMA and, using information in the documents from the French which showed how the Grundstellung indicator system worked, he was able in about a month to develop a theoretical method for recovering wheel wirings based on the fact that message settings (of the three wheels) were enciphered twice to produce the six-letter indicator sent at the beginning of a message (this was the Grundstellung indicator system).

Unfortunately, the amount of work needed to carry out the calculations was prohibitive (and might be prohibitive even with modern computers). Then Rejewski was given two more documents that had been provided by France, these containing two monthly schedules of daily settings (wheel orders, Grundstellung wheel settings used for enciphering message settings, and plug board connections). At this time, wheel orders were being changed only every three months, but by luck the two months provided by the German source fell in two different quarters. All this information permitted the theory to be simplified sufficiently for Rejewski to recover wirings of the three wheels and reflector by the end of December, 1932.

The ENIGMA as it was at that time looked like this:



There were three 26-point wired wheels which could be inserted into the machine in any order (but not backwards). There was a reflector (Umkehrwalze) which had input-output contacts on only one side that were connected to each other in pairs. Each wheel had one notch on it which controlled the stepping of the wheels. The fast wheel, F, advanced one position for each encipherment of a letter; the medium wheel, M, did not advance for an encipherment unless either F advanced off of its notch or unless M itself was at its own notch, in either of which events M advanced one position. The slow wheel, S, did not advance for an encipherment unless M advanced off of its notch, in which case S advanced one position. The reflector, U, did not step during encipherment of a message (and in fact was not settable). The stecker between the "maze" and the input-output mechanisms could be changed by the operator but remained constant during the encipherment of a message; it consisted at this time of 14 points connected straight through and 12 points exchanged in pairs.

In addition to all these variables, the alphabet ring on each wheel (by which the wheel could be set in a specified position at the beginning of a message) was rotatable relative to the core of the wheel and could be put at any one of 26 offsets. Thus, setting the wheels so that the same letters appeared at the bench marks would produce different settings of the wirings themselves if the alphabet ring offsets (Ringstellung) were different. Once all these variable elements were appropriately set up, the code clerk typed each plain text letter in turn and, for each one, wrote down as cipher text the letter which lit up. Depressing the key also caused the wheels to advance appropriately.

In July, 1939, the British and French were informed of the Poles' success on ENIGMA and GC & CS (later renamed GCHQ) accelerated its own partly successful work against it, [158]. ENIGMA was used by the German Army, Air Force, and Navy, among other government elements. Although rather heavy, it was small enough for one person to carry and it operated from batteries, so it was suitable for field use. The Germans continually improved their usage of ENIGMA by changing wheel and reflector wirings a number of times; by increasing the number of available wheels from which daily wheel orders could be selected (they went from three to five to eight in the course of time); by changing the indicator system several times; by increasing the number of steckered letters from 12 to 20; by devising nonreciprocal steckers; and eventually by building a four-wheel ENIGMA (for Navy use) which included a pluggable and replaceable reflector, [233].

At one point, Germany undertook, with some reluctance, to fulfill Japan's request for several hundred ENIGMAs, [104], [221]. They did not want to provide their best models, and after supplying Japan with some 185 machines they found that these versions would be insecure if used as Japan planned to employ them, [21]. They therefore dragged their feet and Japan did not get the number it wanted. Whether for this reason or not, Japan did build at least some ENIGMAs of its own design, [23].

Reference [233] gives an outline of the known uses of ENIGMA and of some other wired wheel machines as of March, 1945, and of attacks against them.

Appendix III: TUNNY (see [11])

TUNNY was an on-line teleprinter scrambler developed by Germany during the second World War. There were three models, SZ-40, SZ-42A, and SZ-42B; SZ stands for Schluesselzusatzgeraet, which means "cipher teleprinter attachment". All three models produced five-bit key characters which were added (level-by-level modulo 2) to plain text characters presented in the form of International Baudot Code (that is, five bits per character). Each level of key was the sum of two bits read from two different wheels, a different pair of wheels for each level of key. Five of the ten wheels involved, one for each level, stepped regularly one position per encipherment. The other five all stepped one position after an encipherment or all stood still, depending on bits read from a "motor" wheel and from other sources (the three TUNNY models had different sources for additional motion control bits). The British called the five regularly-stepping wheels "Chi wheels", the five hesitating wheels "Psi wheels", and the two wheels involved in motion control "Mu wheels".

The Chi wheels had respectively 41, 31, 29, 26, and 23 "pins" and were paired, in order, with Psi wheels having respectively 43, 47, 51, 53, and 59 pins. One Mu wheel had 61 pins and the other had 37 pins. The 61-wheel stepped one position for every character enciphered, and the 37-wheel stepped one position if the 61-wheel had an operative pin at its current setting but did not step if the 61-wheel had an inoperative pin. The Psi wheels stepped one position (in unison) if the 37-wheel had an inoperative pin and if the other sources summed to 1 modulo 2 (an operative pin is assumed to have value 1, an inoperative one value 0). The TUNNY models used these other sources for motion control:

SZ-40 -- no other source;
SZ-42A -- the 31-wheel pin from the previous encipherment, or else that value plus level 5 of plain text two encipherments back;
SZ-42B -- the previous 31-wheel pin plus the 43-wheel pin from the previous encipherment, or else that sum plus level 5 of plain text two back.

The British referred to the use of plain text in motion control as "autoclave" (nowadays we would use the term "plain text autokey").

[redacted]

[redacted]

Reference [11] gives an excellent account of TUNNY history, German Naval usage of it, the cryptanalytic methods developed to exploit it, and the organization of the British efforts against it.

Appendix IV: Hagelin Machines

Boris Hagelin, a Swede, began inventing and producing cipher machines as early as 1927, [12], and eventually established the company now called Crypto AG and located in Zug, Switzerland. A hand machine called A-22 of 1927 vintage was followed in 1928 by models B-13, B-21, and B-22 of an electric machine that incorporated fractionation, three pin wheels (of lengths 17, 19, and 21), and two half-Hebern wired wheels; in 1930 by the B-31/32 which were improved models of B-21/22; in 1932 by the B-211, a further improvement; and in 1935, 1936, 1937, and 1938 by the C-35, C-36, C-37, and C-38, respectively. The C-series machines were the "letter-subtractor" machines of which the C-38 became a huge commercial success, [19], and which the U.S. adapted for field use during WW II under the nomenclature M-209 (Army), [30], and CSP-1500 (Navy).

The C-38 is an off-line mechanical hand-operated machine which produces numerical key values in the range 0 to 25 and subtracts from them, modulo 26, the plain text, in which the 26 letters are represented by values 0 to 25. The results are converted back to the letters A to Z and printed on a narrow gummed paper tape that can be torn into short strips and pasted onto a sheet of paper. Key is produced by the interaction of six pin wheels having lengths 26, 25, 23, 21, 19, and 17 with a 27-bar "cage" in which each bar has "lugs" which can be placed opposite any of the wheels. Pin patterns and lug settings are cryptovariables that remain fixed during encipherment of a message. A crank is operated manually to encipher a letter. It causes the cage to rotate so that each bar in turn passes the current pin of each wheel. A lug passing an "active" pin on some wheel pushes its bar to the left thus contributing a value of one to the key value. That is, the key value is the total number of bars displaced during a rotation of the cage. The crank also causes each wheel to advance one position so that new pins are ready for the next encipherment. There is in addition a feature called the "slide" that can be set by the operator to any one of 26 values but which remains fixed during encipherment. The enciphering equation can therefore be written as PLAIN + CIPHER = KEY + SLIDE, modulo 26, [81].

Hagelin also made electric keyboard models designated BC-38 as well as C-38 versions for other alphabet sizes, and some versions with mixed print wheels (i.e., letters A to Z were associated with numbers 0 to 25 in a scrambled order), [27]; these were not changeable, however, as were the mixed print wheels for some later models. In addition, he designed a variety of one-time-tape key generators and teleprinter cipher machines, but the C-38 was the real workhorse.

[redacted]

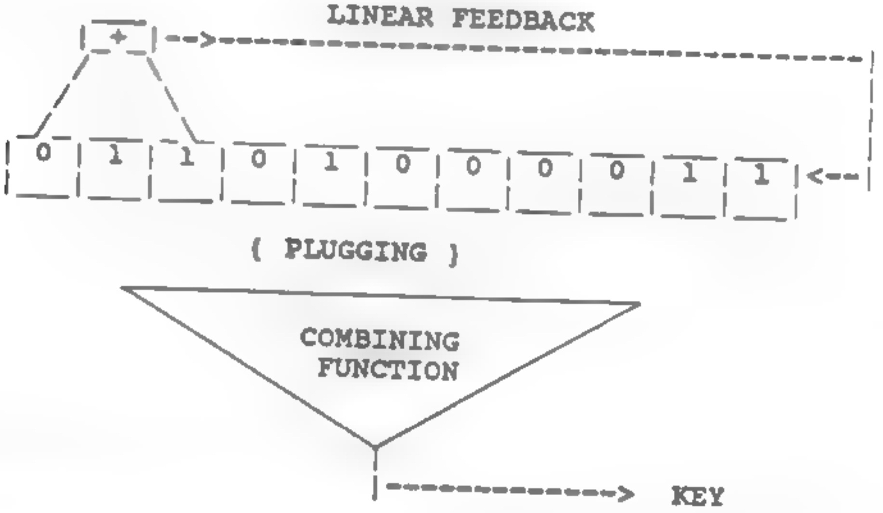
(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P L 86-36

[redacted]

Appendix V: Electronic Cipher Machines

One of the desireable properties for a cipher machine is that it should produce a key stream (or a sequence of wheel positions, or of machine states) that does not cycle; i.e., does not repeat over and over. Since it is impossible for a deterministic machine not to cycle, the next best thing is for it to have a very long cycle, preferably longer than the total number of characters expected to be enciphered before cryptovariables are changed. In the case of electromechanical cipher machines, which typically employed banks of wired wheels or pin wheels, long cycles were obtained by selecting rules of motion that guaranteed this. For electronic cipher machines, linear feedback shift registers with feedback logic guaranteeing maximal cycle lengths are usually employed.

Here is a much simplified representation of the classical model of U.S. electronic cipher machines:



It produces one key bit per step, and a step consists of: reading out the contents or "fill" of the register (consisting of bits); permuting them via the plugging for input into the combining function which then computes the key bit; calculating the feedback bit; and then shifting each bit one position (or "stage") to the left. The leftmost bit is discarded while the feedback bit is inserted into the rightmost stage. If the "feedback function" is properly chosen, successive register fills will run through all possible n-bit patterns before repeating. It has been found mathematically that feedback logic to accomplish this must be somewhat more complicated than the simple linear logic shown in the example, but that there are linear feedback functions for every length register that will cause it to produce each n-bit pattern except all 0's before repeating. In such cases the cycle length is $(2^n)-1$.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3) P L 86-36

The cryptovariables for a machine like the example are the particular plugging chosen and the initial contents of the register. The plugging merely selects (or "taps") certain stages of the register to provide inputs to specific variables of the "combining function", a Boolean function which uses the selected bits from successive register fills to calculate a key bit. The combining function is usually a permanent part of the machine and is designed to produce a key stream that looks as random as possible. [redacted]

More realistic electronic cipher machines use more than one register, adding the output of the nonlinear combining function of one register to the feedback bit of another or using it to control how many steps another takes between key bits. Many variations are possible, but it is more difficult than one would think to avoid weaknesses that could open the door to exploitation by an enemy cryptanalyst. Reference [88] is an excellent source of information about the history of U.S. electronic cipher machine developments.

[redacted]

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P L. 86-36

[redacted]

[redacted]

Appendix VII: Public Key Systems

Before about 1970 there were a few American nongovernment mathematicians who were interested in cryptology, some even to the extent of carrying out research in it over a period of years; [2], [145], and [155] are examples. However, public cryptology really came to life in 1976 with the publication of "New Directions in Cryptography" by Diffie and Hellman, [86], although that paper was clearly the result of earlier research on the part of the authors. (Their interest in cryptology had come to the attention of NSA somewhat earlier when Hellman objected strongly to the Data Encryption Standard (DES), [9].) One of the ideas in "New Directions" that caught the imagination of many mathematicians and computer scientists around the world was what the authors called "public key cryptography", an idea that had been put forth internally by James Ellis in 1970, [92], under the appellation "nonsecret encryption".

Encryption can be expressed abstractly as the transformation of a plain text message into a cipher message under the control of a key. In classical cryptographic systems, the transformation is usually fairly simple: for instance, the key may determine the starting point in a long sequence of "random" numbers which are to be added to the sequence of plain text values, the result being a sequence of cipher values. To decrypt, the same sequence of random values, starting at the same point, must be subtracted from the cipher sequence. The random sequence and the key (starting point) must therefore be available to both the sender and the receiver of the message, but not to anyone else. The transformation (addition) is simple and can easily be undone by subtraction.

In contrast, public key encryption uses some much more complicated transformation, one that is "easy" to perform with any specified key but can be undone only with a different key (this decryption key must obviously be related to the encryption key). The idea is that the transformation should be of such a nature that the relation between encryption and decryption keys is so complicated it requires an exorbitant amount of work to calculate one from the other unless one knows some secret ingredient of the relationship. The transformation algorithm itself can be made public as long as the secret ingredient is known only to the receiver of a message; to enable someone to send him a message, the recipient chooses an encryption key, calculates its related decryption key using the secret information that he has about the relationship, and openly sends the encryption key to the message sender. The sender (and possibly everyone else in the world) knows the transformation method and the encryption key and can therefore encrypt a message and send it to the receiver. However, only the receiver can decrypt it because no one else can feasibly determine the decryption key.

Not many transformations suitable for public key cryptosystems have been found so far. The best-known ones are the knapsack system, [163], the RSA system, [194], the exponentiation system, [77], and McEliece's system, [162]. Some variations of these as well as a few other public key cryptosystems are discussed in [55] and [180], with

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

sketches of attacks on most of them. Both the RSA and exponentiation systems were invented internally before their public appearances; C.C. Cocks, [73], devised what is essentially the RSA system, and Rick Proto, [188], had suggested the exponentiation scheme as an "irreversible" transformation, prior to Ellis' paper on nonsecret encryption. No public key cryptosystem has yet been used operationally. [redacted]

A. Knapsacks, [163]

The knapsack public key system is based on the difficulty of solving the following problem: a large number (perhaps 100) of positive integers of various sizes are specified, and someone selects a subset of them, adds up the integers in the subset, and tells you that sum. Your problem is to determine which integers were selected for the subset.

This problem is hard in the sense that no one has succeeded in devising an algorithm guaranteed to solve any such problem (i.e., for any such set of specified integers) with an amount of work depending polynomially on the number of specified integers. There are certain classes of specified sets, though, for which it is easy to solve the problem. For example, suppose the integers a(1), a(2), ..., a(100) have the property that a(1)<a(2), a(1)+a(2)<a(3), ... , and so on up to a(1)+a(2)+...+a(99)<a(100). (Such a set is called superincreasing.) Then if the sum of a subset is S, it is easy to tell whether a(100) was in the subset because S must be less than a(100) if it was not in the subset and S must be greater than or equal to a(100) if it was in the subset. If a(100) is found to be in the subset, subtract it from S to get S'; otherwise, let S' equal S. Then it is easy to tell whether a(99) was in the subset by comparing it with S'. This process can be continued, and will quickly determine the subset whose sum is S.

Merkle and Hellman, [163], suggested that a public key cryptosystem could be based on a superincreasing set of positive integers by transforming it into another set as follows. First choose a modulus, m, that is larger than the sum of all integers in the set, and choose a multiplier x that is relatively prime to m; m, x, and the a's are secret cryptovariables. Then let b(i) be the least positive residue of x*a(i) modulo m, and use the b's as public cryptovariables. To send a message, convert it to binary form by any convenient coding, split it up into blocks of 100 bits each, and use each block in turn to select a subset of the b's according to whether successive bits are 0 or 1. Form the sums of the selected subsets and transmit them as cipher.

The recipient can decrypt (a block at a time) by forming y*S modulo m where S is a sum (cipher) and y is the inverse of x modulo m; only the recipient can determine y because no one else knows x and m. Since S = sum (b(i)*p(i)), where p(i) is the i-th plain text bit of the block, it is true that S is congruent to sum (x*a(i)*p(i)) and therefore y*S is congruent to sum (a(i)*p(i)). But then the problem is one of dealing with a superincreasing set and that is easy. A cryptanalyst, on the other hand, knows only the b's and is therefore faced with a facsimile of the general knapsack problem.

Hellman and Merkle also remarked that one could iterate the transform procedure by choosing another modulus m' larger than the sum of the b's and another multiplier x' relatively prime to m', and taking c(i) to be the least positive residue of x'*b(i). This could be repeated as often as desired. Note, however, that the public cryptovariables (the "knapsack numbers") will get larger and larger, on the average, and therefore the cipher sums will also get larger and larger. In fact, even a single transformation will result in an increase of the average number of cipher bits over the number of plain text bits.

B. RSA, [194]

The so-called RSA public key cryptosystem is based on the difficulty of factoring integers, a process that is known empirically to be laborious but which has not been proved to have any specified degree of difficulty. C.C. Cocks of GCHQ in 1973, [73], suggested a slightly less general version of the RSA system, which did not appear until four years later.

In the RSA system, two large prime numbers p and q (of perhaps 100 digits each) are selected by the recipient to be the secret cryptovariables. The recipient also chooses a number e relatively prime to both p-1 and q-1. The numbers m=p*q and e are the public cryptovariables. To encipher a message, the sender converts it by any convenient means into a sequence of positive integers each less than m. He then raises each of them to the e-th power modulo m and transmits the sequence of powers as cipher. Since the recipient knows p and q, he is able to determine the unique number d for which d*e is congruent to 1 modulo (p-1)*(q-1); he then raises each cipher number to the d-th power modulo m to obtain the sequence of plain text values. If a cryptanalyst were able to factor the publicly available modulus m, then he also could decrypt the message; the assumption is that factoring is too hard.

One drawback to the RSA system is that it requires one to find prime numbers large enough to make factoring infeasible. It is thought that each prime should have in the neighborhood of 100 digits. It might seem to a nonmathematician that finding such primes would itself involve a factoring process, but that is not the case. Testing an integer for primality is much easier than actually finding its factors, and the appearance of RSA in fact stimulated some new ideas which have improved such testing. Public researchers also discovered weaknesses associated with using primes of a certain form in the RSA system, so that finding acceptable ones is somewhat more complicated than merely finding large ones. Of course, performing modular arithmetic with such large numbers demands either multiple precision computer routines or specially designed chips.

C. Exponentiation, [77]

~~SECRET [illegible]~~

The public key cryptosystem based on exponentiation relies for security on the difficulty of finding "logarithms" of elements in finite fields (or, more recently, in groups) [redacted]

Logarithms in finite fields are defined differently from ordinary logarithms. The nonzero elements of a finite field of order p^n may be represented as powers of a primitive element of the field. There is more than one primitive element available, but once one has been selected (called the generator), the logarithm of an element relative to the generator is defined to be the least power to which the generator must be raised to equal the element. The logarithm is unique modulo $(p^n)-1$.

In the exponentiation system, some large finite field $GF(p^n)$ is selected to be the public cryptovariable. To encrypt a message, the sender converts it by any convenient method to a sequence of elements of the finite field. To encipher each value y of the message, he then chooses some exponent e which has an inverse d modulo p^n-1, and transmits to the recipient y^e. The recipient also chooses some exponent g which has an inverse f modulo p^n-1, and transmits back to the sender the field element $(y^e)^g$. The sender forms $((y^e)^g)^d$ which equals y^g and sends that to the recipient who can then calculate $(y^g)^f=y$. Since (e,d) and (g,f) are known only to the sender and recipient, respectively, no one else is supposed to be able to decipher the message y. If a cryptanalyst were able to solve the discrete logarithm problem, however, he could recover e and g, determine d and f, and so decrypt the message.

Note that when p=2, the field elements can be represented as polynomials with coefficients in the field of integers modulo 2, reduced modulo some irreducible polynomial f(x). Assuming that f is primitive, any nonzero polynomial of the field may then be represented as some power of x, and exponentiation can be performed by an appropriate type of linear shift register with feedback polynomial f. This is the connection with the distance problem.

A drawback of the exponentiation public key cryptosystem is that it requires three transmissions (two from sender to receiver, one from receiver to sender) in order to communicate information. Because of this, it seems to be suitable only for short and infrequent messages. In fact, when it first appeared (in [86]) the authors (Diffie and Hellman) proposed it merely for use in establishing the cryptovariables to be used for a conventional cryptographic system.

The idea of using the group of points on an elliptic curve over a finite field, and exponentiating in that group, is receiving some attention at the present time, [165]. Not much is known about it as yet, although elliptic curves are being intensively studied in connection with factoring algorithms as well.

D. McEliece's System, [162]

In this public key cryptosystem, the public key is a large k by n matrix G', where k<n, formed in the following way. First, the recipient chooses a k by n generator matrix G for some Goppa code ([137] contains a definition of Goppa codes and further references for them) with the ability to correct t errors. Then he chooses a random nonsingular k by k matrix S (one with not too many 0 entries) and a random n by n permutation matrix P. The matrices G, S, and P are the secret cryptovariables, and G' is the matrix product S*G*P.

To encipher a message, the sender converts it to a sequence of bits by any convenient means, breaks it up into k-bit segments, and enciphers each segment by considering it as a vector and multiplying it by G', then garbling t randomly chosen bits of the product. That is, the n-bit cipher sequence c is m*G'+e where m is the plain text segment and e is the "error vector".

The recipient deciphers the message by first multiplying c by the inverse of P to get the vector $c*P^{-1}=m*S*G+e*P^{-1}$. He then uses G to "correct" the "errors" the sender deliberately introduced, the result being m*S. Finally, he multiplies this by S^{-1} (i.e., S inverse) to obtain the message m. A cryptanalyst, not knowing S, P, or G (the code), is supposedly unable to decipher the message without expending a prohibitive amount of work.

References

[1] Adleman, L.M., "A Subexponential Algorithm for the Discrete Logarithm Problem with Applications to Cryptography", Proceedings, 20th IEEE Found. Comp. Sci. Symp., 1979, pp. 55-60. (Preprint available, R51 Classified Mathematics Library,S-216378.)

[2] Albert, A.A., "Some Mathematical Aspects of Cryptography", Invited address, American Mathematics Society, 22 Nov 1941, S-16632 (R51 Classified Mathematics Library).

[3] Allen, G.R. et al., "Final Report, HYBERG Project - An Algorithmic Study of an Advanced Flexible Processor System", May 1978, Control Data, Ltd.

[4] Andelman, D., "Maximum Likelihood Estimation Applied to Cryptanalysis", Information Systems Laboratory, Stanford Electronics Laboratories, Department of Electrical Engineering, Stanford University, Dec 1979, S-223331 (R51 Classified Mathematics Library).

[redacted]

[6] Andrew, C., ed., "Codebreaking and Signals Intelligence", Frank Cass & Co. Ltd., 1986 (NSA Main Library).

[redacted]

[9] Anon., "Data Encryption Standard", National Bureau of Standards, FIPS Pub. 46, Jan 1977.

[10] Anon., "GEE WHIZZER", NSA Tech. Journal, Vol. VIII, No. 1, Winter 1963, S-153566 (R51 Classified Mathematics Library). (This may have been written by Frank Rowlett.)

[11] Anon., "General Report on TUNNY", undated but circa 1945, S-127890 (Cryptologic Collection Box 520). (The writing style of technical cryptanalytic parts of this paper is that of I.J. Good.)

[redacted]

b 1
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

[15] Anon., "Historical Study. The National Security Agency Scientific Advisory Board, 1952-1963", NSA Historian (C-317), Sep 1965, S-178195 (FANX Technical Library).

[16] Anon., "History of Navy Attack on LONGFELLOW", OP 202, 14 Dec 1949, S-17364 (R51 Classified Mathematics Library).

[17] Anon., "KEYSMITH System Acquisition Plan", R8, 19 May 1982.

[redacted]

[20] Anon., "Mechanical Principles Involved in Solving the ENIGMA by Machine Methods", undated, S-55499 (Cryptologic Collection Box 60).

[21] Anon., "Message from Berlin, Action Tokyo, 11/151620/I 1943 (TOI 11/17/1943)" (Navy Translation 4/27/44 30513-30523-30533), L-5131 (Cryptologic Collection Box 76).

[redacted]

[23] Anon., "Preliminary Report on the SAPPHIRE Cipher Machine Used in JN-73", RIP-181, OP-20-G, 27 Aug 1945, L-5133 (Cryptologic Collection Box 76).

[24] Anon., "Processing and Analytic Equipment Manual", Feb 1963, S-215821 Part I (FANX Library).

[redacted]

[26] Anon., "SLED", S-32147, May 1953 (R51 Classified Mathematics Library).

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[30] Anon., "The History of Converter M-2090", Historical Section, ACofS, G2, Army Security Agency, Washington, 4 Mar 1952, L-124 (Cryptologic Collection Box 40).

[31] Anon., "Wiring Recovery", ENIGMA Series, RIP 606, Communication Intelligence Technical Paper TS-10/E4, Vol. 4, 30 Aug 1946, S-6236 (Cryptologic Collection Box 69).

[redacted]

[35] [redacted] et al (18 authors), (title omitted), IDA-CRD W.P. No. 290, Apr 1970 (R51 Classified Mathematics Library).

[36] [redacted], "Two Attacks on the KY-1", IDA-CRD W.P. No. 48, May 1962, L-5221 (R51 Classified Mathematics Library). (b)(3)-P.L. 86-36

[37] Berlekamp, E.R., "Algebraic Coding Theory", McGraw-Hill Book Company, 1968 (NSA Main Library).

[redacted]

[44] Bloch, G. (translated by [redacted], "ENIGMA Before ULTRA; Polish Work and the French Contribution", CRYPTOLOGIA, Vol XI, Number 3, July 1987, pp. 142-155 (NSA Main Library).

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[45] Blum, M. and Micali, S., "How to Generate Cryptographically Strong Sequences of Pseudo Random Bits", IEEE 23rd Symp. on Found. of Comp. Sci., 1982, pp. 112-117 (FANX Library).

[redacted]

[redacted]

[47] Box 66 of the Cryptologic Collection contains some papers on NEMA.

[48] Box 73 of the Cryptologic Collection contains some TYPEX material.

[49] Boxes 15 through 21 of the Cryptologic Collection contain many papers dealing with CORAL, JADE, and PURPLE.

[50] Boyar, J., "Inferring Sequences Produced by Pseudo-Random Number Generators", U. of Chicago Tech. Report 86-002, 1986.

[redacted]

[redacted]

[54] Brickell, E., "Are Most Low Density Polynomial Knapsacks Solvable in Polynomial Time?", Proc. 14th Southeastern Conference on Combinatorics, Graph Theory, and Computing, 1983.

[55] Brickell, E.F. and Odlyzko, A.M., "Cryptanalysis: A Survey of Recent Results", Proceedings of the IEEE, Spring 1988, to appear.

[redacted]

[redacted]

[redacted] [58] [redacted] et al, "An Attack on BYTEMAN", SCAMP W.P. No. 35/79, Sep 1979 (R51 Classified Mathematics Library).

[redacted]

[redacted]

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[61] Cairns, S.S., "Report on SCAMP to the Director of the Armed Forces Security Agency", 8 Sep 1952 (R51 Classified Mathematics Library).

[redacted]

U/~~FOUO~~) 66] [redacted] and Silverman, R.D., "Parallel Implementation of the Quadratic Sieve", Journal of Supercomputing, Vol. 2, No. 1, 1988.

[redacted]

[68] Cave, R.L. et al, "Description of the IDA/CRD LAN", IDA-CRD W.P. No. 908, Nov 1987, S-230814 (R51 Classified Mathematics Library).

[redacted]

[70] Chaum, D. et al, eds., "Advances in Cryptology, Proceedings of Crypto 82", Plenum Press, New York and London, 1983 (Q41 files).

[71] Clark, R.W., "The Man Who Broke PURPLE", Weidenfeld and Nicolson, London, 1977 (NSA Main Library).

[redacted]

[73] Cocks, C.C., "A Note on 'Non-Secret' Encryption", HR/TECH.A/279, GCHQ, 20 Nov 1973 (R51 Classified Mathematics Library).

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

[77] Coppersmith, D., "Cryptography", IBM J. Res. Develop., Vol. 31, No. 2, Mar 1987 (NSA Main Library).

[78] Coppersmith, D., "Fast Evaluation of Logarithms in Fields of Characteristic Two", IEEE Trans. Info. Theory IT-30, pp. 587-594, 1984 (NSA Main Library).

[79] Coppersmith, D., Odlyzko, A.M., and Schroeppel, R., "Discrete Logarithms in GF(p)", Algorithmica, Vol. 1, 1986, pp. 1-15.

[80] Davies, D.W. and Parkin, G.I.P., "The Average Size of the Key Stream in Output Feedback Encipherment", Eurocrypt82, 1983, pp. 263-279.

[redacted]

[redacted]

[redacted]

[86] Diffie, W. and Hellman, M.E., "New Directions in Cryptography", IEEE Transactions on Information Theory IT-22, Nov 1976 (NSA Main Library).

[redacted]

[88] [redacted] "A Review of Developmental Cryptography of the United States Government, 1950-1980", R1, (to appear). (This paper is NOFORN.)

[redacted]

[90] [redacted] "On Sorting Large Amounts of Data", A543/002/81/PN, 25 Nov 1981, S-224019 (R51 Classified Mathematics Library).

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

86-36

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

[redacted]

[93] [redacted], "QUANDER", Office of Applications Engineering, 7 Jun 1971, S-200448 (FANX Library).

[94] Fairbanks, S., "Z-Flags", NSA Tech. Journal, Vol. IX, No. 1, Winter 1964, S-182358 (R51 Classified Mathematics Library).

[redacted]

[103] Ford, A.M., "The Birth of ATLAS I", NSA Tech. Journal, Vol. XVIII, No. 1, Winter 1973, S-207051 (R51 Classified Mathematics Library).

[104] Ford, C.A., Cover memo, Subject: "Naval Section Memo No. 60, The Purchase of German ENIGMA Machines by the Japanese Navy", cover memo dated 9 Sep 1944, memo no. 60 dated 7 Mar 1944, S-164830 (Cryptologic Collection Box 73).

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

[106] Friedman, W.F., "Description of the General Principles of an Invention of a Machine for Locating Idiomorphs and Isomorphs in Cryptanalysis", Signal Intelligence Section, 14 Apr 1937, C83.8 (R51 Classified Mathematics Library).

[107] Friedman, W.F., "Six Lectures on Cryptology", 1965, S-144473 (R51 Classified Mathematics Library).

[108] Friedman, W.F., "The Index of Coincidence and Its Applications in Cryptanalysis", Signal Intelligence Section, 1935, C-507 (R51 Classified Mathematics Library).

[109] Friedman, W.F., "L'Indice de Coincidence et Ses Applications en Cryptographie", Riverbank Publication No. 22, Paris, 1921, S-31782 (Cryptologic Collection Box 363).

[redacted]

[111] Garey, M.R. and Johnson, D.S., "Computers and Intractability, A Guide to the Theory of NP-Completeness", W.H. Freeman and Company, 1979 (NSA Main Library).

[redacted]

[redacted]

[114] Gleason, A., "The Theory of Wired Wheels", 28 Jan 1953, S-3058 (Cryptologic Collection Box 78).

[redacted]

U ~~FOUO~~ [118] [redacted] "A List of Properties of Bayes-Turing Factors", IDA-CRD W.R. No. 113, Apr 1964, S-154619 (R51 Classified Mathematics Library).

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

[redacted]

[121] Good, I.J., "Pioneering Work on Computers at Bletchley", A History of Computing in the Twentieth Century, Academic Press, 1980 (NSA Main Library).

[redacted]

[125] Good, I.J., "The Interaction Algorithm and Practical Fourier Series", J. of the Royal Statistical Society, Series B, Vol. 20, No. 2, pp. 361-372, 1958 (also an Addendum in Vol. 22, No. 2, pp. 372-375, 1960); (NSA FANX Library).

[126] Hanrahan, R.B., "Considerations of MARK XII Reply Evaluation Procedure", Doc-21 Informal Note No. 7, 3 Nov 1958 (X Library).

[127] Harris, B., "Probability Distributions Related to Random Mappings", Annals of Math. Stat., Vol. 31, No. 4, Dec 1960, pp. 1045-1062 (FANX Library).

[redacted]

U/~~FOUO~~ [130] [redacted] A542/02/82/R, 1 Sep 1982.

[redacted]

[redacted]

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]

[136] Kendall, M.G. and Babington-Smith, B., "Randomness and Random Sampling Numbers", J. Roy. Stat. Soc. 101, 1938, C-1356 (R51 Classified Mathematics Library).

(b)(3)-P.L. 86-36

U//~~FOUO~~[137] [redacted], "Equivalence Classes of Irreducible Goppa Codes", R51/MATH/03/81, 4 Mar 1981, S-222650 (R51 Classified Mathematics Library).

[redacted]

[redacted]

[139] Knuth, D., "Deciphering a Linear Congruential Encryption", IEEE Transactions on Info. Theory, Vol. IT-31, No. 1, Jan 1985, pp. 49-52 (FANX Library).

(b)(3)-P.L. 86-36

U//~~FOUO~~[140] [redacted], "Probabilistic Motion: An Introductory Survey", SCAMP W.P. No. 71/86, Sep 1986, S-230010 (R51 Classified Mathematics Library).

[141] Kronlage, C.R., "FLEMING Completion Report", R325, Feb 1976, S-213554 (R51 Classified Mathematics Library).

[142] Kullback, S., "Statistical Methods in Cryptanalysis", Signal Intelligence Service, 1938, C-835 (R51 Classified Mathematics Library). (Reprinted in the NSA Technical Literature Series as Monograph No. 14, 1967, S-180494.)

[143] Kullback, S., "The Increasing Complexity of the Analytic Equipment Program", NSA, 12 Oct 1955, S-146406 (R51 Classified Mathematics Library).

[redacted]

[redacted]

[redacted][145] [redacted], "Recent Literature on Algebraic Cryptography", Book Review, NSA Tech. Journal, Vol. VII, No. 2, Spring 1962, S-182292 (R51 Classified Mathematics Library).

[redacted][146] [redacted], "Sorting for COMSEC", S12 Inf. Note No. 280, 15 Jul 1970, S-199570 (R51 Classified Mathematics Library).

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

[148] Lagarias, J.C. and Odlyzko, A.M., "Solving Low-Density Subset Sum Problems", J. of the ACM, Vol. 32, No. 1, pp. 229-246, Jan 1985 (NSA Main Library).

[149] [redacted], "Report on Project SCAMP 1985", Vol. I, Sep 1985, S-227669 (R51 Classified Mathematics Library).

[150] [redacted] "Report on Project SCAMP 1985", Vol. II, Sep 1985, S-227670 (R51 Classified Mathematics Library).

(b)(3)-P.L. 86-36

[151] Leahy, F.T., "Bayes Marches On", NSA Tech. Journal, Vol. V, No. 1, Jan 1960, S-182242 (R51 Classified Mathematics Library).

[152] Leibler, R.A. and [redacted]; "A Brief History of IDA/CRD", RSA-26, 22 Jun 1987, plus Appendices VI-XI, same authors, RSA-27, 22 Jun 1987 (R51 Classified Mathematics Library).

[153] Lenstra, H.W., Jr., "Elliptic Curve Factorization", Annals of Mathematics, Vol. 126, No. 3, Nov 1987, pp. 649-673 (FANX Library).

[154] Lenstra, A.K., Lenstra, H.W., Jr., and Lovasz, L., "Factoring Polynomials with Rational Coefficients", Mathematische Annelen, Vol. 261, No. 4, 1982.

[155] [redacted] et al, "The Application of Mathematics to Cryptology", Research Proposal, 15 May 1969, S-216240 (R51 Classified Mathematics Library).

[redacted]

[158] Mahon, A.P., "The History of Hut Eight, 1939-1945", Jun 1945, S-2453 (Cryptologic Collection Box 65).

[159] Mayol, F.C., "HEMBREE Completion Report", R73, Oct 1966, S-185024 (FANX Library).

[160] [redacted] "General Cryptanalytic Attacks", A583/25/72 Tech. Report, 1 Dec 1972, S-220529 (R51 Classified Mathematics Library).

[161] [redacted] "General Cryptanalytic Attacks Supplement", A541/29/76 Tech. Report, 3 Nov 1976, S-220528 (R51 Classified Mathematics Library).

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

[162] McEliece, R.J., "A Public-Key Cryptosystem Based on Algebraic Coding Theory", DSN Progress Report 42-44, JPL, 1978, pp. 114-116. (Preprint available, R51 Classified Mathematics Library, S-218869.)

[163] Merkle, R. and Hellman, M., "Hiding Information and Signatures in Trapdoor Knapsacks", IEEE Trans. Info. Theory IT-24, Sep 1978, pp. 525-530 (NSA Main Library).

[redacted]

[165] Miller, V.S., "Use of Elliptic Curves in Cryptography", Advances in Cryptology-CRYPTO 85, Springer-Verlag, 1986.

[redacted]

[redacted] [168] [redacted] "The Diagnosis of (name omitted)", IDA-CRD W.P. No. 891, Dec 1987, S-230071 (R51 Classified Mathematics Library).

(b)(3)-P.L. 86-36

[169] Moore, D.P. and Swift, J.D., "Note on Sorting Repeats", SCAMP W.P. No. 12/61, 4 Aug 1961, S-132628 (R51 Classified Mathematics Library).

[170] Moore, D.P. and Swift, J.D., "Further Note on Sorting Repeats", SCAMP W.P. No. 17/61, 9 Aug 1961, S-132632 (R51 Classified Mathematics Library).

[171] Morrison, M.A. and Brillhart, J., "A Method of Factoring and the Factorization of F7", Math. Comp., Vol 29, 1975, pp. 183-205 (NSA Main Library).

[redacted]

[175] Parker, R.D., "Recollections Concerning the Birth of One-Time Tape Cryptography", NSATJ Vol I, No. 2, Jul 1956 (R51 Classified Mathematics Library).

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

[178] [redacted], "The Great SCAMP Contest", SCAMP W.P. No. 28/85, Sep 1985, S-227656 (R51 Classified Mathematics Library).

[179] [redacted], "Report on Project SCAMP 1986", Sep 1986, Vol. I S-230070, Vol. II S-230072 (R51 Classified Mathematics Library).

(b)(3)-P.L. 86-36

[180] Patterson, W., "Mathematical Cryptology for Computer Scientists and Mathematicians", Rowman & Littlefield, USA, 1987 (NSA Main Library).

[181] Pendergrass, J.T., LCDR, "High Speed Digital Computing Machines, Cryptanalytic Use of", Op-20-L-4, 15 Oct 1946, S-1993 (R51 Classified Mathematics Library). (Reprinted in NSA Tech. J., Vol. IX, No. 3, Aug 1964.)

[182] [redacted], "RYE: An Extended Capacity Remote Access System", NSA Tech. Journal, Vol. IX, No. 2, May 1964, S-182368 (R51 Classified Mathematics Library).

[redacted]

[186] Pohlig, S.C. and Hellman, M., "An Improved Algorithm for Computing Logarithms Over GF(p) and Its Cryptographic Significance", IEEE Trans. Info. Theory IT-24, 1978, pp. 106-110 (NSA Main Library).

[187] Pomerance, C., "The Quadratic Sieve Algorithm", Advances in Cryptology: Proceedings of Crypto 84, Springer-Verlag, Berlin, 1985, pp. 169-182 (NSA Main Library).

[redacted]

[189] [redacted], "Project NYLAND System Acquisition Plan and System Plan", R&1, 25 Aug 1978.

[190] Randell, B., "The Colossus", A History of Computing in the Twentieth Century, Academic Press, 1980 (NSA Main Library).

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[191] Reeds, J.A. and Weinberger, P.J., "File Security and the UNIX System Crypt Command", AT&T Bell Laboratories Technical Journal, Vol. 63, No. 8, Oct 1984, pp. 1673-1683 (NSA Main Library).

[192] Rejewski, M., "Mathematical Solution of the ENIGMA Cipher", Zastosowania Mathematyki, Applicationes Mathemalire, 1980, S-223330 (R51 Classified Mathematics Library); (reprinted in Cryptologia, Vol. 6, No. 1, January, 1982).

[193] Rivest, R.L., "The Impact of Technology on Cryptography", MIT Laboratory for Computer Science, undated (but received at NSA in May 1978), S-216310 (R51 Classified Mathematics Library).

[194] Rivest, R.L., Shamir, A., and Adleman, L., "On Digital Signatures and Public-Key Cryptosystems", MIT/LCS/TM-82, M.I.T., Apr 1977, S-218461 (R51 Classified Mathematics Library).

[redacted] [redacted]

[196] Rueppel, R.A., "Analysis and Design of Stream Ciphers", Springer-Verlag, 1986 (NSA Main Library).

[redacted] [197] [redacted] "Topics in Cryptologic Mathematics", R51, to appear in the NSA Cryptologic Literature Series.

[198] Schnorr, C.P. and Lenstra, H.W., Jr., "A Monte Carlo Factoring Algorithm with Linear Storage", Math. Comp., Vol. 43, No. 167, Jul 1984, pp. 289-311 (NSA Main Library).

(b)(3)-P.L. 86-36

[199] Seaman, J.N., "Solution of the German Teletypewriter Cipher System ('TUNNY')", Jun 1947, S-264 and S-9060 (S-264 in R51 Classified Mathematics Library).

[redacted] [200] [redacted], "Common Repeat Searching Methods", SCAMP W.P. No.2/80, Sep 1980, S-221938 (R51 Classified Mathematics Library).

[redacted] [201] [redacted], "Sorting on the CRAY-1: An Overview", SCAMP W.P. No. 16/78, Sep 1978, S-219499 (R51 Classified Mathematics Library).

[redacted] [redacted]

[203] Shamir, A., "A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem", Proceedings of the 23rd Annual Symp. on the Found. of Comp. Sci. (IEEE), pp. 145-152, 1982 (NSA Main Library).

[204] Shamir, A., "On the Complexity of Knapsack Systems", M.I.T., Feb 1979, S-216344 (R51 Classified Mathematics Library).

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

[redacted] [206] [redacted] A541/48/77/IN, Oct 1977.

(b)(3)-P.L. 86-36

[207] Silverman, R.D., "The Multiple Polynomial Quadratic Sieve", Mathematics of Computation, Vol. 48, pp. 329-339, 1987 (FANX Library).

[208] Simmons, G.J. and Holdridge, D., "Forward Search as a Cryptanalytic Tool Against a Public-Key Privacy Channel", Proceedings, 1982 IEEE Symposium on Security and Privacy, Oakland, CA, 26-28 Apr 1982, pp. 117-128.

[209] Snyder, S.S., "Earliest Applications of the Computer at NSA", NSA Tech. Journal, Vol. XVIII, No. 1, Winter 1973, S-207051 (R51 Classified Mathematics Library).

[210] Snyder, S.S., "Famous First Facts, NSA Part I: Pre-Computer Machine Cryptanalysis", NSA Tech. Journal, Vol. XVII, No. 4, Fall 1972, S-205540 (R51 Classified Mathematics Library).

[211] Snyder, S.S., "History of NSA General-Purpose Electronic Digital Computers", Monograph No. 2, NSA Technical Literature Series, 1964, S-157337 (R51 Classified Mathematics Library).

[redacted]

[214] Stahly, G.F., [redacted]

[215] Stahly, G.F., "Assessment of HUNDON", P1/159/86, 9 Apr 1986 (cover memo for attached paper on HUNDON by [redacted]

[redacted]

[219] Stahly, G.F., The Cryptography of STURGEON", NSA-712, 15 Jul 1954, S-32532 (R51 Classified Mathematics Library).

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[220] Taussky, O. and Todd, K., "Generation and Testing of Pseudo-Random Numbers", Symposium on Monte Carlo Methods, H.A. Meyer, ed., Wiley, New York, 1956, pp. 15-28 (NSA Main Library).

[221] Taylor, T., Memo for Colonels Clarke and Corderman, Subject: "Early 'E' History", 22 Jan 1944, S-3091 (Cryptologic Collection Box 73).

[222] Tomash, E., "The Start of an ERA: Engineering Research Associates, Inc., 1946-1955", A History of Computing in the Twentieth Century, Academic Press, 1980 (NSA Main Library).

[redacted]

[redacted]

[225] Tutte, W.T., "The Analysis of Rectangles", 22 Feb 1945, Collected Papers on Mathematical Cryptology, Vol. II, pp. 399-404, (R51 Classified Mathematics Library).

[redacted]

[redacted]

[227] West, N., "GCHQ", Weidenfeld & Nicholson Limited, London, 1986 (NSA Main Library).

[228] Western, A.E. and Miller, J.C.P., "Tables of Indices and Primitive Roots", Royal Society Math. Tables, Vol. 9, Cambridge Press, England, 1968 (NSA Main Library).

[229] Wheatley, L.H., "Cryptanalytic Machines at NSA", NSA-34, 30 May 1953, S-183840 (FANX Library).

[redacted]

[redacted]

[redacted] [232] [redacted] "Optical Corralation - The FLEMING Approach", Tech. Memo R51/77, 15 Nov 1971, S-204003 (FANX Library).

[233] Wray, W.D., "ENIGMA Conferences -- Tentative List of ENIGMA and Other Machine Usages", OP-20-G4-A, 30 Mar 1945, S-2607 (Cryptographic Collection Box 67).

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

[235] Yates, F., "The Design and Analysis of Factorial Experiments", Tech. Comm. No. 35 of the Commonwealth Bureau of Soils, Hampden, England, 1937, S-202795 (R51 Classified Mathematics Library).

[236] [redacted] "An Introduction to Cryptologic Mathematics: Probability and Statistics", NSA Technical Literature Series Monograph No. 10, 1966, S-169303 (R51 Classified Mathematics Library). (Reprinted from lectures given by [redacted] over the years.)

[redacted]

[239] Zorpette, G., "Electrotechnology in World War II: Breaking the enemy's code", IEEE Spectrum, Vol. 24, No. 9, pp. 42-51, Sep 1987 (NSA Main Library).

(b)(3)-P.L. 86-36
(b)(6)

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Index

b (1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(1),
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(6)

(b)(3)-P.L. 86-36

(b)(1)
P.L. 86-36 50 USC 3605

(b)(6)

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(6)

(b)(1)
(b)(3)-P.L. 86-36

(b)(6)

(b)(3)-P.L. 86-36

(b)(6)

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36
(b)(6)

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

Doc ID: 6649792

~~CONFIDENTIAL~~

DISTRIBUTION

DIR	1
D/DIR	1
C/S	1
DDI	1
DDO	1
DDPP	1
DDR	1
DDT	1
ADT	1
ADDI	1
ADDO	1
ADDR(T)	1
A	1
A5	1
A51	2
A52	2
A53	4
A54	4
B	1
B8	4
CCS [redacted]	1
G	1
G [redacted]	1
G03	4
G4	1
G41	4
G42	4
G43	4
G44	4
G45	4
G46	4
G2	1
G5	1
G6	1
G9	1
P1	2
P1 [redacted]	50
P11	2
P12	4
P13 [redacted]	2
P13 [redacted]	1
P15 [redacted]	4
P15 [redacted])	1
Q3 ([redacted]	1
Q41	1
R/MA [redacted]	1
R5	1
R5 (for SRC)	1
R51	1
R51 (for CRD)	1
R511	2
R512	2
R513	2
R53	2
R56	4
R8	1
SUSLO	1
SUSLO-2	1
T3	1
T4	1
T442	1
T51 [redacted]	1
[redacted]	1
[redacted]	4
W3	1
W346	2
X	1
X1	4
X2	2
X3	2
Y07	2
Z (Stahly)	22

(b)(3)-P.L. 86-36

~~CONFIDENTIAL~~

~~Not Releasable To Contractors~~

~~LACONIC~~

THIS DOCUMENT CONTAINS CODEWORD MATERIAL